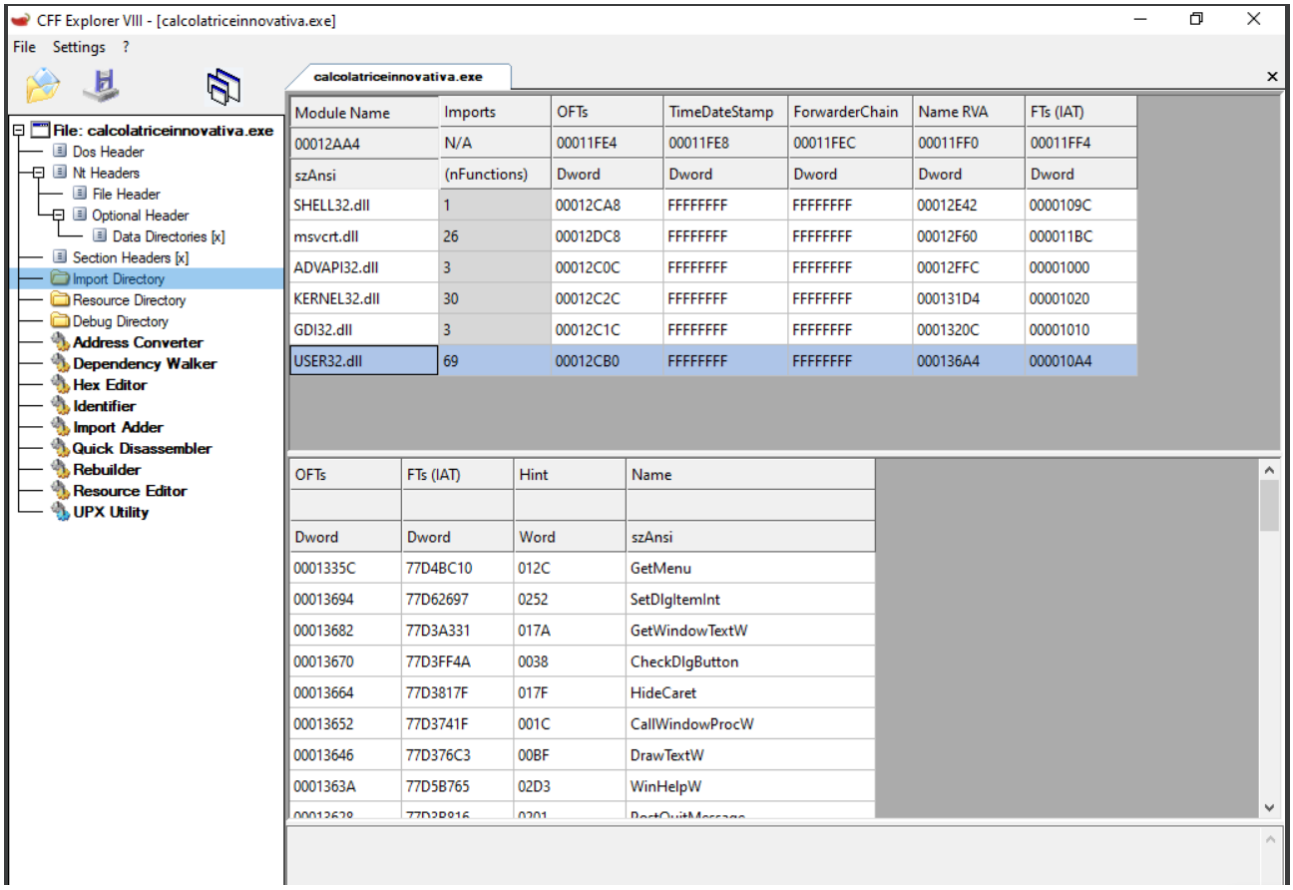
W21D4



Import Directory, vengono mostrati i moduli o le librerie (DLL) che questo eseguibile importa.

SHLWAPI.dll è una libreria di sistema di Windows, il cui nome sta per **Shell Lightweight Utility Library**. È utilizzata principalmente per fornire funzioni utili per la gestione di operazioni comuni nei programmi che interagiscono con il sistema operativo, in particolare con il file system e la shell di Windows (l'interfaccia grafica).

Alcune delle funzionalità offerte da **SHLWAPI.dll** includono:

1. **Gestione stringhe**: funzioni per la manipolazione delle stringhe di testo, come concatenazione, ricerca e formattazione.
2. **Operazioni su URL**: strumenti per l'analisi, combinazione e manipolazione degli URL.
3. **Interazione con il registro di sistema**: funzioni per leggere, scrivere e gestire chiavi del registro di Windows.
4. **Funzioni di confronto e ricerca**: utili per confrontare file o identificare tipi di dati.

Questa libreria è spesso utilizzata da applicazioni di Windows per eseguire operazioni di utilità legate alla gestione di file, URL e stringhe, riducendo la necessità per gli sviluppatori di implementare queste funzionalità da zero.

msvcrt.dll (Microsoft Visual C Runtime Library): Questa DLL contiene le funzioni runtime della libreria C di Microsoft, utilizzate per fornire funzioni di base come la gestione di memoria,

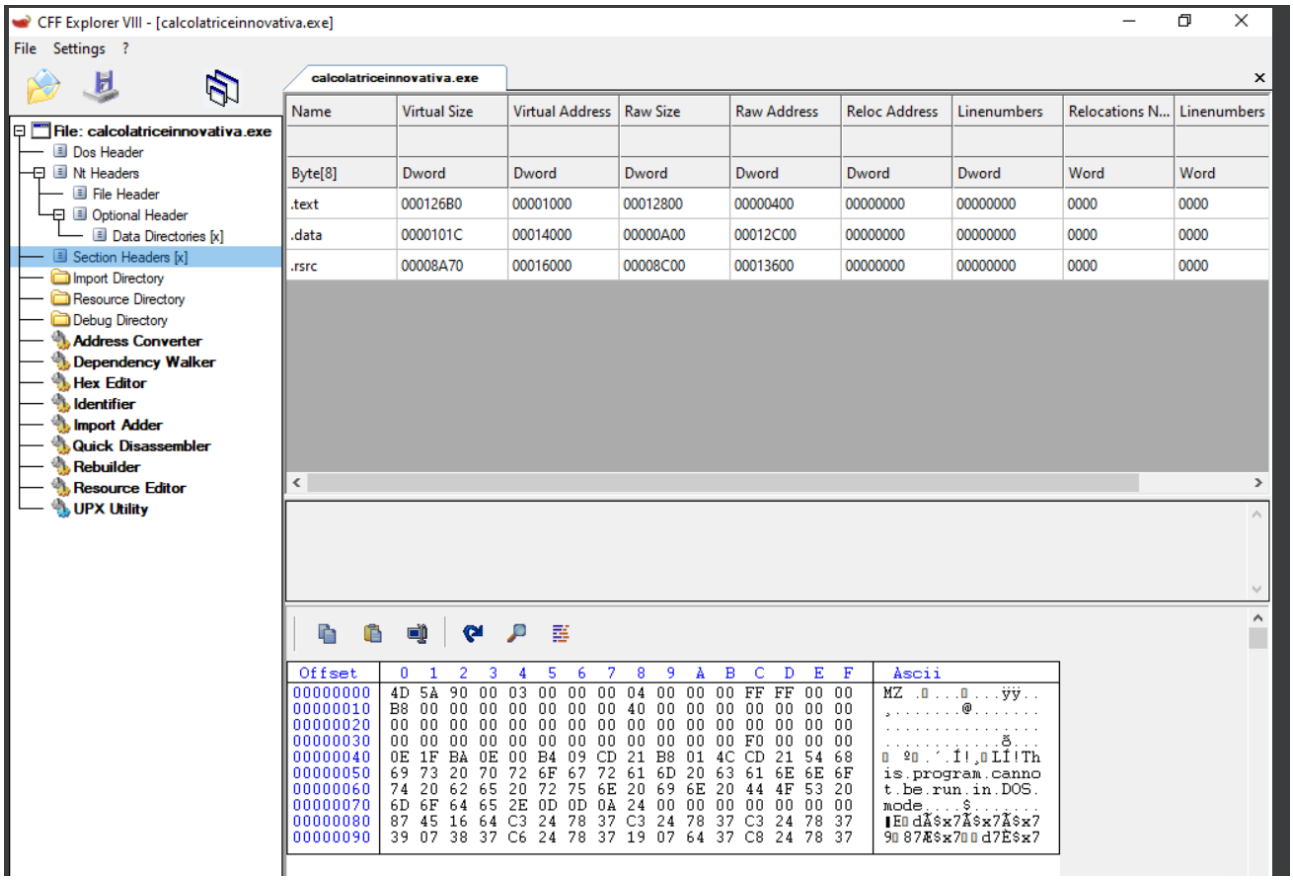
l'I/O (input/output), la gestione di stringhe, funzioni matematiche e altro. È utilizzata da molte applicazioni sviluppate con Visual C++.

ADVAPI32.dll (Advanced API Library): Fornisce un insieme di API avanzate per Windows, utilizzate per funzioni legate alla sicurezza, gestione del registro di sistema, gestione dei servizi e altre funzionalità di basso livello relative all'amministrazione e alla sicurezza del sistema operativo.

KERNEL32.dll (Windows Kernel API Library): Questa libreria contiene la maggior parte delle funzioni di base del sistema operativo Windows, incluse la gestione della memoria, gestione dei processi e dei thread, gestione dell'I/O, operazioni su file e altro. È una delle DLL fondamentali per il funzionamento di Windows.

GDI32.dll (Graphics Device Interface): Fornisce funzioni grafiche per Windows, consentendo alle applicazioni di disegnare su schermo o su altri dispositivi di output. Include operazioni per il disegno di linee, forme, testo e immagini. Viene utilizzata per la grafica bidimensionale nelle applicazioni.

USER32.dll (Windows User Interface API): Contiene le funzioni per gestire gli elementi dell'interfaccia utente, come finestre, bottoni, caselle di testo e altri controlli. Include anche funzioni per la gestione dei messaggi di Windows, l'interazione con tastiera e mouse e la gestione delle finestre.



1. **Name**: Il nome della sezione. Ci sono tre sezioni elencate:
    - `.text`: La sezione che contiene il codice eseguibile (le istruzioni della CPU).
    - `.data`: Contiene i dati statici e variabili globali utilizzate dal programma.
    - `.rsrc`: La sezione che contiene le risorse del programma (icone, immagini, stringhe di testo, ecc.).
2. **Virtual Size**: La dimensione virtuale della sezione in memoria. Indica quanto spazio occupa questa sezione quando viene caricata in memoria.
3. **Virtual Address**: L'indirizzo di memoria virtuale in cui la sezione sarà caricata quando il programma viene eseguito.
4. **Raw Size**: La dimensione effettiva della sezione nel file eseguibile.
5. **Raw Address**: L'indirizzo all'interno del file eseguibile dove la sezione inizia.
6. **Reloc Address e Reloc Number**: Indicano informazioni sulla riallocazione degli indirizzi, che sono necessari quando un modulo o DLL viene spostato in una posizione di memoria diversa da quella predefinita. In questo caso, non ci sono informazioni sulla riallocazione (valori a zero).

Parte inferiore (Hex e Ascii):

Nella parte inferiore della finestra, puoi vedere il **Dump Hexadecimale** del file, ovvero una rappresentazione in formato esadecimale dei dati presenti nel file eseguibile. Ogni byte del file è rappresentato sia in forma esadecimale che in forma ASCII (a destra).

Il dump inizia con "MZ", che è la firma di un file eseguibile di Windows (indica che è un file in formato DOS/Windows PE). La parte in ASCII mostra un messaggio classico: **"This program**

cannot be run in DOS mode", che appare nei file eseguibili di Windows per indicare che non possono essere eseguiti su vecchi sistemi DOS senza interfaccia grafica.